ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

ENHANCING DATA COMPLIANCE IN THE UNITED STATES HEALTHCARE SYSTEM: ADDRESSING CHALLENGES IN HIPAA AND HITECH ACT IMPLEMENTATION

Adewale Samuel Osifowokan[1], Zeliatu Ahmed[2], Tobias Kwame Adukpo[3] Nicholas Mensah[4]

[1]School of Medicine, Stony Brook University, USA.
[2] College of Business and Information Systems, Dakota State University | Madison, SD
[3] Department of Accounting, University for Development Studies, Ghana
[4]Department of Accounting, University of Ghana.

Article DOI: https://doi.org/10.36713/epra21263
DOI No: 10.36713/epra21263

ABSTRACT

This study explores the challenges of data compliance in the U.S. healthcare system, focusing on the implementation of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The aim is to identify gaps in the regulatory frameworks and propose solutions to enhance compliance in the context of rapid technological advancements. A qualitative methodology was employed, incorporating case studies, industry reports, and academic literature to analyze vulnerabilities in healthcare data security and evaluate the effectiveness of existing regulations. Findings indicate that although HIPAA and HITECH have established a strong foundation for protecting Personal Health Information (PHI), they increasingly fail to address modern challenges such as cloud computing, internet of things (IoT) integration, and cybersecurity threats. Systemic barriers, including resource constraints, inconsistent standards, and insufficient technical expertise, further increase the risks of noncompliance. Despite federal initiatives like the HITRUST framework providing enhanced guidance, these efforts require greater adaptability to meet the demands of evolving healthcare IT infrastructures. The study concludes that advancing data compliance necessitates a multifaceted approach, including revising regulatory frameworks, fostering interdisciplinary collaboration, and developing a skilled workforce proficient in healthcare cybersecurity. The researchers argue that these measures will strengthen PHI protection, foster innovation in healthcare delivery, and ensure a secure and compliant healthcare ecosystem.

KEYWORDS: *Data compliance, HIPAA, HITECH Act, healthcare system, data security, privacy, regulatory challenges, United States*

INTRODUCTION

The US healthcare sector, with its $5 trillion valuation (Mohammed, 2017; Osifowokan et al., 2025), faces growing data compliance challenges despite strict regulatory frameworks. The 2014 Anthem BC/BS breach, which compromised 80 million patients' PHI, exemplifies the vulnerability of healthcare systems even under HIPAA protection. The incident highlighted fundamental gaps in data security that persist despite federal regulations designed to protect patient information.

The digital transformation of healthcare through EHR systems, CPOE, and IoT integration has created a complex compliance landscape (Mohammed, 2017). While these technological advances have modernized healthcare delivery, they have also expanded the attack surface for cybercriminals (Dodi, 2021; Mallick & Nath, 2024; Agbadamasi et al., 2025). Singh et al. (2016) noted that "The transition from paper records to interconnected digital systems, cloud computing, and mobile devices has introduced new vulnerabilities that existing regulations struggle to address effectively".

The regulatory framework itself has significant limitations. HIPAA, enacted in 1996, requires updates to address emerging technologies (Subramanian et al., 2024). Current compliance standards may not fully account for modern healthcare IT infrastructure, leaving security gaps. This issue is further complicated by the rapid pace of technological change, which often outstrips regulatory updates.

The complexity of digital transformation in healthcare adds to the compliance burden. According to Ganiga et al. (2020), the integration of EHR systems with external networks and cloud services has created intricate data flows that must be secured and monitored. Additionally, the rise of connected medical devices and IoT implementations, along with the increased use of personal devices in healthcare settings, has created a more complex security environment than ever before.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Cybersecurity threats continue to evolve, becoming more sophisticated and targeting interconnected healthcare systems (Umoren et al., 2025). Organizations face the challenge of protecting interconnected systems while maintaining necessary accessibility for healthcare providers and patients. This delicate balance between technological advancement and data protection requires a more adaptive approach to compliance.

These challenges highlight the urgent need to revise and strengthen current compliance frameworks to better protect PHI while supporting technological innovation in healthcare. The future of healthcare security depends on developing flexible, comprehensive regulations that keep pace with evolving technology while ensuring robust patient data protection.

LITERATURE REVIEW

U.S. Healthcare Data Compliance Concerns

To minimize data security risks, U.S. healthcare providers must ensure their employees receive proper training on data protection protocols. Past security breaches, such as the 2014 attack on Boston Children's Hospital by the hacktivist group Anonymous and the recent malware breach at Merck, highlight the importance of preparedness (Munyolo, 2021). These incidents underscore the need for continuous evolution in security practices to match the rapid advancement of technology (Umoren et al., 2025; Adebayo et al., 2025). However, Sadri (2024) notes that current regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), often lag technological progress. Since its enactment in 1996, HIPAA has undergone limited updates and primarily focuses on what must be protected rather than providing specific security measures (Subramanian et al., 2024). The law lacks clear guidelines on emerging technologies, such as firewalls, wireless networks, and cloud security, which were not widely used when the legislation was introduced. While HIPAA mandates that healthcare organizations protect patient health information and secure their systems from unauthorized access, it does not provide detailed frameworks for how to address modern threats. This gap points to a broader issue in the industry: to effectively safeguard healthcare data, HIPAA regulations must be revised to align with current technological standards and emerging security challenges.

A notable trend across industries is the increasing financial investment in cybersecurity. A 2017 HIMSS survey of the healthcare industry revealed that 71% of organizations allocate a portion of their budget to cybersecurity, with the average spending accounting for over 3% of their total budget. Healthcare organizations are investing more in cybersecurity compared to previous years, primarily focusing on hiring additional security professionals and enhancing overall security (Abraham et al., 2019; Umoren et al., 2025). This reflects the growing recognition that cybersecurity is not just an IT issue but a business-essential concern. Historically, healthcare security has been largely viewed through the lens of HIPAA compliance, specifically meeting the requirements of the Security and Privacy Rules. When asked about their top security priority, employees overwhelmingly cited risk assessments (Choi & Williams, 2022; Snell, 2017; Agbeve et al., 2025). In the past, healthcare CEOs and executives took a more passive stance on cybersecurity, but today, these concerns are a central focus, signaling a shift in mindset. Businesses now understand that a cyberattack can severely impact their financial stability and have taken a more proactive role in preventing such threats (Safitra et al., 2023; Adukpo et al., 2025; Adebayo et al., 2025).

Another emerging trend is the adoption of alternative cybersecurity frameworks by healthcare providers (Bhuyan et al., 2020). Opie (2024) states that "The National Institute of Standards and Technology (NIST) has developed a framework that complements HIPAA, filling the gaps where HIPAA falls short". Because HIPAA lacks detailed security guidelines, NIST introduced the PROTECT function, which assesses patient data security and emphasizes employee education and awareness. This function ensures that healthcare staff understand their role in maintaining cybersecurity. The NIST framework highlights that data protection is a shared responsibility involving both technology and human factors at every organizational level (Whitman & Mattord, 2016; Rohan et al., 2023; Amoako et al., 2025).

To effectively address cybersecurity challenges, the healthcare industry must adopt a collaborative approach. Financial constraints should not hinder cybersecurity advancements, particularly as patient data is shared across multiple providers and third-party vendors. Protecting both large and small healthcare organizations is critical in ensuring system-wide security. If cybersecurity is truly a priority, industry competition should not obstruct progress. Only through collective cooperation can meaningful improvements be achieved (Conaty-Buck, 2017).

U.S. Healthcare Data Compliance Challenges

The healthcare industry faces significant challenges in ensuring compliance with data protection regulations. While healthcare providers are entrusted with sensitive patient data, many fail to implement the proper tools and programs to ensure their protection. They employ primarily trained personnel to focus on cybersecurity, but also require the sharing of sensitive data across different systems to ensure patient safety while also keeping the information secure and unmodified. A major issue in healthcare compliance arises from the varying requirements for different subsets of the industry (Dash et al., 2019). These subsets, including pharmacies, hospitals, and medical device companies, each have unique compliance issues. For example, a medical device company may need patient data for the operation of its device, but does not need to retain that data long-term. The system must, therefore, be designed in a way that allows for the secure and effective removal of this data once it is no longer needed. There is a wide variety of special-purpose computers used in medical devices, many of which could potentially put patients at risk (Andre, 2017). In the medical device sector, personal medical devices such as glucose monitors and heart monitors collect large amounts of data about individuals. These devices often use low-power Bluetooth connections to connect to apps on smartphones,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

creating a pathway into the device that could be exploited to gain access to other parts of the system. To ensure compliance with privacy requirements, medical device manufacturers must ensure their devices are not vulnerable to exploitation (Andre, 2017).

Argaw et al. (2020) underscored that "Pharmacies encounter unique challenges compared to hospitals and doctors' offices when it comes to data security". Pharmacies track the prescriptions they fill, requiring their databases to be secure, complete, and unaltered. Staff must also be properly trained in maintaining patient privacy. Given that a list of prescribed medications can reveal significant health information, pharmacies must prevent accidental disclosures of medical treatments. Since prescriptions are often collected by individuals other than the patient, pharmacies need to ensure that the person picking up the medication is authorized to do so. Failure to verify this can result in the unauthorized dispensing of controlled substances or medications, leading to the exposure of a patient's medical diagnosis and significant privacy violations (Andre, 2017).

Doctors' offices, which are typically smaller businesses, also face unique data compliance challenges (Tanner, 2017). Due to limited budgets, smaller practices may lack the resources to adequately secure patient information, leaving it vulnerable to compromise. With the increasing shift toward electronic health records (EHRs), cybersecurity costs for smaller practices are rising. Many smaller offices may lack dedicated IT staff, which could result in outdated or unnecessary software and hardware that is vulnerable to attacks (Damar et al., 2024; Umoren et al., 2025; Agbadamasi et al., 2025). It is crucial for these offices to periodically review their installed software and hardware and remove obsolete systems that are no longer receiving updates, as these create vulnerabilities. While smaller practices often lack the funds for custom security solutions, they can still meet HIPAA compliance by implementing affordable off-the-shelf cybersecurity tools and training employees in best practices. This cost-effective approach helps mitigate risks by focusing on employee education and resource management (Lanz, 2016).

According to research by Javaid, et al. (2023), "Larger medical practices, which often involve multiple doctors, face distinct cybersecurity concerns compared to smaller practices". These larger offices typically operate more advanced systems that share information across the practice. As more medical devices are connected to networks, both wired and wireless, it becomes important to implement robust security measures to safeguard the network (Chaudhary & Hamilton, 2016). With numerous doctors and staff members using portable devices, including those taken home, these practices must prioritize ensuring all devices are up-to-date and secure, especially when accessed through external networks. Additionally, the systems must be hosted in secure locations and encrypted properly, particularly for practice with multiple offices in different geographic areas, which require accessing data over the open internet. Another significant aspect of larger practices is ensuring proper access controls are in place, restricting unauthorized users from accessing sensitive information, and minimizing potential attack vectors.

Hospitals and medical centers, which often host external doctors for surgeries, tests, and other procedures, face unique challenges in cybersecurity compliance (Wasserman & Wasserman, 2022). These institutions must protect patient data while allowing external users, who may not be employees of the center, access to necessary systems and information. The challenge lies in managing access for a large, diverse group of users who require varying levels of data access but may not frequently use the center's network. These institutions need to ensure that, while granting the necessary access, they also protect their network and patient data from potential breaches. As external contractors often have elevated, remote, or physical access rights, it is easy for organizations to lose track of all those with access (Douglas, 2015). To maintain compliance, hospitals must regularly audit user access, deactivate inactive accounts, and adjust access privileges to reduce security risks and ensure compliance with healthcare data regulations.

Data Compliance Issues in the U.S Insurance Companies

Insurance companies in the United States face significant challenges in complying with data protection regulations due to the large volume of sensitive data they handle. As custodians of comprehensive patient data, including medical records, prescriptions, health diagnoses, employment information, and personal identifiable data, insurance companies are prime targets for cyberattacks (Ntantogian et al., 2021). In many cases, insurance providers are the sole digital record keepers for patients, especially when primary care providers do not utilize electronic medical records. Thapa et al. (2021) noted that "This centralized storage of relevant information makes it essential for insurance companies to implement stringent security measures, such as encryption, to protect patient data from breaches". Although insurance companies do not need to grant as many users access to their systems as healthcare facilities do, the sheer volume of data they store necessitates robust cybersecurity measures to prevent breaches.

Similarly, insurance research organizations, whether public or private, face significant concerns regarding patient privacy and cybersecurity compliance. These organizations often collect data for clinical trials or research studies that go beyond typical medical information. This data may include details about lifestyle, medications, and daily health progress, which are vital for the success of the research. However, research entities may struggle to maintain the necessary data security measures, particularly when the study is part of a larger institution with inconsistent data protection protocols. Ensuring confidentiality is especially important when research results are later shared in public forums, as revealing too much about a participant could compromise their privacy. To mitigate these risks, research entities must ensure that the data remains both secure and accessible for research purposes, as emphasized by Shoffner et al. (2013), who highlight the importance of balancing data security

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

with usability. Additionally, these organizations must have processes in place to prevent the unintentional release of identifiable data, which could violate patient privacy and regulatory standards.

Data Security Compliance Issues in the U.S. Healthcare Sector

The primary regulation governing privacy and security in the U.S. healthcare sector is the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA aims to protect personal health information (PHI) from unauthorized disclosure, ensuring patient confidentiality (Moore & Frye, 2019). The law requires healthcare providers to safeguard PHI, particularly as electronic health records (EHRs) have become more prevalent in the digital age (Rechtman & Rashbaum, 2015). Despite its importance, HIPAA has limitations, as it lacks specific guidance on the extent of protection required for PHI, leading to ambiguity around how institutions should implement cybersecurity measures. While some progress has been made in securing information through individual medical personnel, external cyberattacks pose significant threats, which often target IT systems rather than medical staff. This disconnect between IT and healthcare professionals, combined with insufficient investments in cybersecurity, has made the healthcare sector vulnerable to cyber threats.

Additionally, the National Institute of Standards and Technology (NIST) framework has become increasingly important in guiding data compliance practices within the healthcare sector. Initially designed for federal agencies, NIST standards have been adopted by private healthcare organizations as well (Shackelford et al., 2015). Like HIPAA, NIST's focus is on securing EHRs, both in storage and during transmission, and includes guidelines on encryption, privacy protections, and digital signatures. Moreover, NIST emphasizes meaningful use (MU) and usability, expanding its regulations to cover not only EHRs but also medical devices (Cohen, 2016). However, confusion persists, particularly among vendors who are uncertain about which standards to follow. Many vendors borrow standards from other industries, develop their own, or attempt to comply with various certification requirements like the Certification Commission for Healthcare Information Technology (CCHIT), leading to inconsistencies in healthcare IT security practices. This confusion highlights the challenges faced by the healthcare sector in implementing effective data protection and compliance frameworks (Osifowokan et al., 2025).

In anticipation of the nationwide adoption of electronic health records (EHRs), the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to incentivize the use of EHRs (Gold & McLaughlin, 2016). This law played an important role in addressing the previously vague regulations by specifying situations that required enhanced security measures and detailing how to protect sensitive systems and data. HITECH also tackled the issue of lax enforcement by holding healthcare providers accountable for security breaches resulting from "willful neglect" (Gold & McLaughlin, 2016). For providers aiming to receive incentives or avoid penalties, it became essential to increase their understanding of HIPAA's Privacy and Security Rules, along with the new provisions introduced by HITECH (Shoffner et al., 2013).

Following the enactment of HITECH, the Health Information Trust Alliance (HITRUST) was established to create the Common Security Framework (CSF), a certification process for healthcare organizations. Moreover, the Health Care Industry Cybersecurity Task Force, founded by Congress and authorized by the Cybersecurity Act of 2015, publishes an annual report identifying vulnerabilities and collaborates with HITRUST to recommend improvements to the cybersecurity framework and policies (Rechtman & Rashbaum, 2015).

One of the key issues in healthcare technology regulation is the conflict between the U.S. Food and Drug Administration (FDA) and the U.S. Federal Trade Commission (FTC), particularly regarding mobile health devices (mHealth) and wireless technologies. These technologies not only store medical data but are also integral to treatment, raising concerns about the security of devices that are vulnerable to cyberattacks. Striking a balance between ensuring the proper functioning of these devices and protecting patient privacy has become a complex challenge. For example, wireless pacemakers that monitor heart rate and other anomalies via the internet can be compromised by hackers, presenting significant risks to patient safety (Cohen, 2016).

Despite some jurisdictional disagreements between the FDA and FTC, both agencies are working together to raise regulatory awareness, including through an online tool that helps identify the relevant laws for new applications. In addition, HIPAA, HITECH, and the FTC all require healthcare organizations to notify individuals if their PHI is compromised due to a security breach, including incidents involving EHRs. The use of unsecured mHealth devices undermines patient trust in healthcare providers and can lead to both economic and reputational harm (Cohen, 2016).

The necessity of data compliance regulations in the healthcare sector is becoming increasingly evident (Osifowokan et al., 2025; Umoren et al., 2025). A significant challenge in regulating electronic health records (EHRs) has been the reluctance or inability of certain offices and organizations to adopt them. To encourage EHR implementation, the U.S. government introduced the HITECH Act, which offers incentives for its use. While the regulations could benefit from greater specificity, the ultimate responsibility for compliance lies with healthcare organizations to hire or appoint qualified personnel to lead their data compliance efforts. Bridging the gap between IT departments and medical staff is relevant so that everyone is aligned with current regulations and understands the importance of safeguarding patient health information (PHI). Whether adopting the NIST framework, HITRUST's CSF, or another approved system, healthcare organizations must take responsibility for ensuring compliance with these regulations to be effective. For instance,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

while federal regulations mandate the appointment of privacy and information security officers within covered entities, this has not been universally or effectively implemented across the healthcare industry (Schulke, 2017). Thus, ensuring adherence to existing regulations remains a critical challenge for healthcare stakeholders.

Table 1: Systematic Analysis of Literature on Cybersecurity in Healthcare

Author(s)	Year	Methodology	Theory (if any)	Findings
Abraham et al.	2019	Qualitative case study	Organizational resilience theory	Identified persistent cybersecurity vulnerabilities in US healthcare and emphasized the need for leadership engagement.
Andre	2017	Conceptual analysis	Risk management theory	Emphasized cybersecurity as an enterprise-wide risk, requiring executive-level governance.
Argaw et al.	2020	Literature synthesis and expert consultation	N/A	Highlighted cybersecurity risks in hospitals and proposed a multi-stakeholder framework to address systemic vulnerabilities.
Bhuyan et al.	2020	Policy review and recommendations	N/A	A recommended shift from reactive to proactive cybersecurity strategies in healthcare.
Chaudhary & Hamilton	2016	Professional insights and audit review	N/A	Outlined the internal audit's essential role in identifying and mitigating cybersecurity threats in healthcare organizations.
Cohen	2016	Quantitative study on EHR adoption	N/A	Found that HITECH incentives increased EHR adoption but revealed ongoing security and privacy challenges.
Conaty-Buck	2017	Policy commentary	N/A	Emphasized the importance of protecting healthcare records from cyber threats through robust policy and education.
Damar et al.	2024	Theoretical discussion	N/A	Explored AI's growing influence on healthcare cybersecurity and conceptualized new threat dimensions.
Dash et al.	2019	Literature review	N/A	Reviewed how big data in healthcare introduces both opportunities and heightened security risks.
Dodi	2021	Legal and technical analysis	N/A	Analyzed COVID-19's impact on cybersecurity practices, highlighting legal ambiguities and increased vulnerabilities.
Douglas	2015	Conceptual framework development	N/A	Proposed frameworks for identifying threat sources and enhancing cybersecurity posture in healthcare.
Ganiga et al.	2020	System architecture proposal	N/A	Developed a security framework for cloud-based EHR systems focused on encryption and user authentication.
Gold & McLaughlin	2016	Policy analysis	N/A	Evaluated HITECH Act outcomes and highlighted persistent gaps in secure EHR implementation.
Javaid et al.	2023	Comprehensive literature review	N/A	Synthesized practices and trends, identifying integration gaps and future directions in healthcare cybersecurity.
Lanz	2016	Professional recommendations	N/A	Advocated for layered defenses and staff awareness to protect against healthcare data breaches.
Mallick & Nath	2024	Review article	N/A	Surveyed recent cyber-attacks, calling for global strategies and real-time threat intelligence in healthcare.
Mohammed	2017	Regulatory review	N/A	Outlined U.S. healthcare cybersecurity regulations, noting gaps in enforcement and data breach responses.
Moore & Frye	2019	Policy analysis	N/A	Reviewed HIPAA's provisions on security and privacy, detailing challenges in modern healthcare environments.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Munyolo	2021	Legal and regulatory critique	N/A	Critically analyzed Kenya's e-health regulatory landscape, proposing a more cohesive cybersecurity framework.
Ntantogian et al.	2021	Technical review	N/A	Detailed healthcare cybersecurity threats and evaluated current technical countermeasures.
Opie	2024	Case study	N/A	Investigated IBM FHIR server flaws under the 21st Century Cures Act, recommending security hardening practices.
Rechtman & Rashbaum	2015	Legal review	N/A	Clarified misinterpretations and compliance issues surrounding the HIPAA Security Rule.
Rohan et al.	2023	Mixed-methods analysis	N/A	Mapped human and organizational factors to the NIST framework to improve cybersecurity resilience.
Sadri	2024	Legislative commentary	N/A	Called for the modernization of HIPAA to reflect contemporary digital threats and privacy needs.
Schulke	2013	Legal analysis	N/A	Discussed the regulatory challenges of mobile health applications and evolving agency roles.

The review presented in the table above demonstrates the multifaceted nature of cybersecurity challenges within the healthcare sector, as examined through various methodological approaches and disciplinary perspectives. The studies collectively highlight a consistent concern for persistent vulnerabilities, regulatory gaps, and the need for organizational adaptation in the face of evolving threats. Although theoretical framing is limited, with only a few contributions, such as Abraham et al. (2019) and Andre (2017) grounding their analyses in established theories like organizational resilience and risk management, the broader body of work leans heavily on empirical reviews, policy analyses, and conceptual insights. The integration of artificial intelligence, the proliferation of electronic health records, and the adoption of cloud-based solutions are identified as both opportunities and sources of heightened risk (Okonkwo et al., 2025; Osifowokan & Adukpo,2024). Notably, the literature emphasizes the significant role of leadership engagement, intersectoral collaboration, and proactive governance in safeguarding health information systems. Taken together, these contributions underscore the need for holistic, forward-looking cybersecurity frameworks that align with both technological advancements and healthcare policy imperatives.

CONCLUSION

The rapid advancement of technology has brought both advantages and challenges to the U.S. healthcare system. While technological innovations have increased efficiency and improved patient care, they have also heightened vulnerabilities to cyberattacks. One of the persistent challenges facing the healthcare industry is maintaining compliance with federal regulations. Noncompliance often arises not from intentional disregard but due to various systemic challenges, such as insufficient tools and programs to protect sensitive data, inconsistent standards across different sectors, and budget constraints. These factors contribute to the difficulty healthcare organizations face in adhering to data compliance regulations.

Regulations like HIPAA mandate the protection of patient health information (PHI) but often lack detailed guidance on implementing robust security measures. Progress has been made with the introduction of the HITECH Act and the development of the HITRUST framework, which provides incentives and clearer guidelines for establishing strong cybersecurity protocols in the healthcare sector. These initiatives demonstrate federal efforts to enhance the industry's cybersecurity posture and data compliance capabilities.

However, achieving widespread compliance requires more than additional regulations. It necessitates the development of a new generation of skilled IT professionals who understand both the complexities of data compliance and the unique priorities of the healthcare industry. Through fostering collaboration between data compliance experts and healthcare practitioners, the industry can effectively address data compliance challenges and safeguard sensitive patient information in the United States.

REFERENCES

1. *Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.*
2. *Adebayo, O., A, N., Adukpo, T. K. (2025). Navigating Liquidity Management Challenges in the Era of Digital Banking in the United States. World Journal of Advanced Research and Reviews, 25(2), 2711-2719. https://doi.org/10.30574/wjarr.2025.25.2.0576*
3. *Adebayo, O., Mensah, N., Adukpo, T. K. (2025). Beyond Cash Flow Management: How Machine Learning and Scenario Planning Drive Financial Resilience. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 81-89. https://doi.org/10.36713/epra20503*
4. *Adukpo, T. K., & Mensah, N. (2025). Financial technology and its effects on small and medium-scale enterprises in Ghana: An Explanatory Research. Asian Journal of Economics, Business and Accounting, 25(3), 268-284. https://doi.org/10.9734/ajeba/2025/v25i31709*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

5. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). The Role of Business Intelligence in AI Ethics: Empowering U.S. Companies to Achieve Transparent and Responsible AI. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 8-14. https://doi.org/10.36713/epra20314*
6. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). Artificial Intelligence Governance in U.S. Corporations: Legal and Ethical Implications for Business Intelligence and Regulatory Compliance. International Journal of Research Publication and Reviews, 6(3), 3083-3089.*
7. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). Navigating the Intersection of U.S. Regulatory Frameworks and Artificial Intelligence: Strategies for Ethical Compliance. World Journal of Advanced Research and Reviews, 25(3), 969-979. https://doi.org/10.30574/wjarr.2025.25.3.0814*
8. *Agbeve, V., Adukpo, T. K., Mensah, N., Appiah, D., Atisu, J. C. (2025). Comparative Analysis of Digital Banking and Financial Inclusion in the United States: Opportunities, Challenges, and Policy Implications. Asian Journal of Economics, Business and Accounting, 25(3), 452-467. https://doi.org/10.9734/ajeba/2025/v25i31722*
9. *Amoako, E.K.W., Boateng, V., Ajay, O., Adukpo, T.K., Mensah, N. (2025). Exploring the Role of Machine Learning and Deep Learning in Anti-Money Laundering (AML) Strategies within the U.S. Financial Industry: A Systematic Review of Implementation, Effectiveness, and Challenges. Finance & Accounting Research Journal, 7(1). https://doi.org/10.51594/farj.v7i1.1808*
10. *Andre, T. (2017). Cybersecurity is an enterprise risk issue. Healthcare Financial Management, 71(2), 40-46.*
11. *Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10.*
12. *Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of Medical Systems, 44, 1-9.*
13. *Chaudhary, R., & Hamilton, J. (2016). Internal Audit's Critical Role in Cybersecurity. New Perspectives on Healthcare Risk Management, Control & Governance, 35(2).*
14. *Cohen, M. F. (2016). Impact of the HITECH financial incentives on EHR adoption in small, physician-owned practices. International Journal of Medical Informatics, 94, 143-154.*
15. *Conaty-Buck, S. (2017). Cybersecurity and healthcare records. American Nurse Today, 12(9), 62-64.*
16. *Damar, M., Özen, A., & Yılmaz, A. (2024). Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptually. Journal of AI, 8(1), 61-82.*
17. *Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and prospects. Journal of Big Data, 6(1), 1-25.*
18. *Dodi, C. (2021). Cyber Security's New Challenges under the Covid-19 Pandemic: Between Technique and Law. Studii Juridice Universitare, 35.*
19. *Douglas, P. C. (2015). Cyber Risk Management: Do You Know Your Threat Sources? Add more precision to your security framework. New Perspectives on Healthcare Risk Management, Control & Governance, 34(3).*
20. *Ganiga, R., Pai, R. M., & Sinha, R. K. (2020). Security framework for cloud-based electronic health record (EHR) system. International Journal of Electrical and Computer Engineering, 10(1), 455.*
21. *Gold, M., & McLaughlin, C. (2016). Assessing HITECH implementation and lessons: 5 years later. The Milbank Quarterly, 94(3), 654-687.*
22. *Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016.*
23. *Lanz, J. (2016). Bolster your data defenses. Journal of Accountancy, 222(2), 22.*
24. *Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyberattacks, emerging trends, and recent developments. World Scientific News, 190(1), 1-69.*
25. *Mohammed, D. (2017). US healthcare industry: Cybersecurity, regulatory, and compliance issues. Journal of Research in Business, Economics and Management, 9(5), 1771-1776.*
26. *Moore, W., & Frye, S. (2019). Review of HIPAA, part 1: history, protected health information, and privacy and security rules. Journal of nuclear medicine technology, 47(4), 269-272.*
27. *Munyolo, G. N. O. (2021). Cyber-security in E-health: a Critical Analysis of the Regulatory Framework in Kenya (Doctoral dissertation, University of Nairobi).*
28. *Ntantogian, C., Laoudias, C., Honrubia, A. J. D., Veroni, E., & Xenakis, C. (2021). Cybersecurity threats in the healthcare domain and technical solutions. In Handbook of Computational Neurodegeneration (pp. 1-29). Cham: Springer International Publishing.*
29. *Opie, C. A. (2024). Exploring Security Vulnerabilities in FHIR Server Implementations: A Case Study on IBM's FHIR Server in the Context of the 21st Century Cures Act (Master's thesis, University of Hawai'i at Manoa).*
30. *Osifowokan, A. S., Agbadamasi, T. O., Adukpo, T. K., Mensah, N. (2025). Regulatory and Legal Challenges of Artificial Intelligence in the U.S. Healthcare System: Liability, Compliance, and Patient Safety. World Journal of Advanced Research and Reviews, 25(3), 949-955. https://doi.org/10.30574/wjarr.2025.25.3.0807*
31. *Rechtman, Y., & Rashbaum, K. (2015). HIPAA Security Rule-Demystified. CPA Journal, 85(4).*
32. *Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., & Pal, D. (2023, December). Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the NIST cybersecurity framework. In Proceedings of the 13th International Conference on Advances in Information Technology (pp. 1-16).*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

33. *Sadri, M. (2024). HIPAA: A Demand to Modernize Health Legislation. The Undergraduate Law Review at UC San Diego, 2(1).*
34. *Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.*
35. *Schulke, D. F. (2013). The regulatory arms race: Mobile-health applications and agency posturing. BUL Rev., 93, 1699.*
36. *Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int' 'l LJ, 50, 305.*
37. *Shoffner, M., Owen, P., Mostafa, J., Lamm, B., Wang, X., Schmitt, C. P., & Ahalt, S. C. (2013). The secure medical research workspace: an IT infrastructure to enable secure research on clinical data. Clinical and translational science, 6(3), 222-225.*
38. *Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.*
39. *Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient Health Record Protection Beyond the Health Insurance Portability and Accountability Act: Mixed Methods Study. Journal of Medical Internet Research, 26, e59674.*
40. *Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient Health Record Protection Beyond the Health Insurance Portability and Accountability Act: Mixed Methods Study. Journal of Medical Internet Research, 26, e59674.*
41. *Tanner, A. (2017). Our bodies, our data: how companies make billions selling our medical records. Beacon Press.*
42. *Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 129, 104130.*
43. *Umoren, J., Adukpo, T. K., & Mensah, N. (2025). Leveraging Artificial Intelligence in Healthcare Supply Chains: Strengthening Resilience and Minimizing Waste. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(2), 190-196. https://doi.org/10.36713/epra20385*
44. *Umoren, J., Korang, A., Utomi, E., Adukpo, T. K., Mensah, N. (2025). The Importance of Utilizing Big Data Analytics in U.S. Healthcare Supply Chain Management. EPRA International Journal of Multidisciplinary Research, 11(3), 411-421. https://doi.org/10.36713/epra20572*
45. *Umoren, J., Adukpo, T. K., Mensah, N. (2015). Exploring factors, outcomes, and benefits in supply chain finance: Insights and future directions for the U.S. healthcare system. World Journal of Advanced Research and Reviews, 25(02), 060-071. https://doi.org/10.30574/wjarr.2025.25.2.0345*
46. *Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 4, 862221.*
47. *Whitman, M. E., & Mattord, H. J. (2019). Management of information security. Cengage Learning.*
48. *Okonkwo, F. C., Akonor, B. G., & Adukpo, T. K. ARTIFICIAL INTELLIGENCE IN HEALTHCARE SUPPLY CHAIN MANAGEMENT: ENHANCING RESILIENCE AND EFFICIENCY IN US MEDICAL SUPPLY DISTRIBUTION. https://doi.org/10.36713/epra19901*
49. *Osifowokan, A. S., & Adukpo, T. K. (2024). The importance of quality assurance in clinical trials: Ensuring data integrity and regulatory compliance in the US pharmaceutical industry. https://doi.org/10.30574/wjarr.2024.24.3.3652*